



**STRATEGY
RESEARCH
PROJECT**

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

ROLE OF THE CHIEF INFORMATION OFFICER

BY

LIEUTENANT COLONEL BOBBY L. MCKINNON
United States Army

DISTRIBUTION STATEMENT A:
Approved for Public Release.
Distribution is Unlimited.

SENIOR SERVICE COLLEGE FELLOW
AY01



U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

20010712 071

USAWC STRATEGY RESEARCH PROJECT

ROLE OF THE CHIEF INFORMATION OFFICER

by

Lieutenant Colonel Bobby L. McKinnon
U.S. Army

Mr. David Birdwell
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

DISTRIBUTION STATEMENT A:

Approved for public release.
Distribution is unlimited.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: LTC Bobby McKinnon

TITLE: Role of the Chief Information Officer

FORMAT: Strategy Research Project

DATE: 10 April 2000

PAGES: 24

CLASSIFICATION: Unclassified

Organizations are rushing to modify their existing business processes to take advantage of the benefits offered by technology. These organizations are also realizing the increasingly strategic value of their information technology resources; as a result, they have begun to create executive positions known as the Chief Information Officer (CIO). In many of these organizations, the CIO is charged with the responsibility of overseeing information technology resources from an enterprise perspective. In 1996, the President signed what has become known as the Clinger-Cohen Act. It required major Federal Agencies to establish the position of CIO. As the Army embarks on transforming itself into a force that is more deployable, more lethal, and more sustainable, it also becomes more dependent on information technology. This paper identifies the stated roles of the CIO, and identifies several areas that require additional emphasis. These areas include developing a greater sense of ownership for information technology resources, synchronizing the change processes associated with operating and maintaining its information management systems, and providing a common information technology infrastructure.

TABLE OF CONTENTS

ABSTRACT	iii
TABLE OF CONTENTS	v
ROLE OF THE CHIEF INFORMATION OFFICER	1
IMPETUS FOR THE CIO	2
CREATION OF THE CIO ORGANIZATION	3
THE ARMY CIO	4
ROLES AND RESPONSIBILITIES	5
CHANGES SINCE IMPLEMENTATION	6
ROLE OF THE CIO IN COMMERICAL ORGANIZATIONS	7
LESSONS FROM CIVILIAN PRACTICES	8
IMPLICATIONS OF CURRENT IT POLICIES ON TRANSFORMATION	9
CURRENT IT POLICIES	10
CROSS FUNCTIONAL OWNERSHIP	10
CENTRALIZED PLANNING, CONTROL, AND RESOURCING	11
COMMON IT INFRASTRUCTURE	12
CONCLUSION	13
ENDNOTES	15
BIBLIOGRAPHY	17

Role of the Chief Information Officer

The old adage, "if it isn't broken don't fix it," may no longer be true. On any given day, one can find a number of previously successful companies that are on the verge of falling by the wayside. For a variety of reasons, these organizations fail to recognize the changes in their external environment. They fail to understand the changes occurring around them. They fail to identify strategies to counter their competitors' advantages. They fail to understand how new technologies can be used to enhance their own capabilities. They ultimately fail to see the need for change.

The Army has suffered from many of the same failings during its 225 years. At times it has been comfortable with the status quo and has all too often - particularly since the end of the Cold War - been placed in situations for which it was ill-prepared. In some cases (some would argue many cases) the Army did not have the right organizational structures, the right equipment, or the right capabilities. But, unlike organizations on the verge of collapse, the Army and its leadership recognized the need for change.

In their October 12, 1999 announcement to the Association of the United States Army, Secretary of the Army Louis Caldera and the Army Chief of Staff Gen Shinseki unveiled a new vision for the Army. A vision that described a "force that is more deployable, agile, versatile, lethal, survivable, sustainable and dominant at every point along the spectrum of operations . . . We will begin to immediately transform the entire Army into a more dominant and strategically responsive force."¹ In many ways, this vision describes a force that is very much different from today's Army. The "Vision's goal is to ensure that the Army fulfills its Title 10 responsibilities in continuously meeting the National Military Strategy."²

With the unprecedented pace of technical innovation it is a certainty that the strategic environment in the first half of the 21st century will be very much different from that of the Cold War Era and will require an Army very different from the Army of today. It will require a land force that can initiate actions on its own terms, capable of retaining the initiative, building momentum, and winning decisively at every point along the spectrum of operations.

As a result of recognizing the need to reshape the Army, senior leaders of the Army developed a plan to transform it. The transformation plan is focused in three major areas: sustaining the legacy force, creation of an interim force, and developing the objective force.

While there are a number of questions surrounding each of these three forces, there are also a number of similarities. Each force is dependent on force multipliers such as information

dominance, greater lethality, increased survivability, and highly skilled soldiers. Technological innovation and its adaptation is the defining ingredient for each of the force multipliers the Army (and DoD in general) hopes to harness. Accordingly, one of the Army's key leaders associated with enabling information dominance and technology adaptation is the Army's Chief Information Officer (CIO).

The remainder of this paper will focus on the Army's CIO. Specifically this paper will examine the impetus for the creation of the CIO position, restate the roles and responsibilities of the CIO (as documented in the various legislation and pertinent policy documents), identify and assess the changes made within the Army as a result of implementing the corresponding policy, assess similar situations/conditions found in commercial industry, and offer potential lessons to be learned.

Impetus for the CIO

"This era will be one of accelerating technological change. Critical advances will have enormous impact on all military forces. Successful adaptation of new and improved technologies may provide great increases in specific capabilities. Conversely, failure to understand and adapt could lead today's militaries into premature obsolescence and greatly increase the risks that such forces will be incapable of effective operations against forces with high technology."

— JOINT VISION 2010

Organizations are rushing to modify their existing business processes to take advantage of the perceived benefits offered them by implementing information technology solutions. The Department of Defense (DoD), and specifically the Army, are also following suit. "In FY01 the Army will spend 24 percent of its appropriated budget on research and modernization efforts."³ Information technology components will be a significant portion of the budget expenditures.

The question at hand is, "What benefits will the Army realize from those expenditures?" History has repeatedly reminded the information technology community that the actual results of a development or modernization effort are often very much different than the intended ones. "In its 1995 study, the Standish Group estimated that \$81 billion would be spent on software projects that would eventually be canceled and an additional \$59 billion would be spent on software projects that were behind schedule."⁴ Unfortunately, much of the Standish Group's prediction was correct and the trend continues. As a result, many organizations found themselves asking why their IT project failed. The research has shown IT projects fail for a variety of reasons that have both technical and managerial causes. As a result, organizations

are reviewing their internal IT management structures, processes, and procedures in an attempt to improve the success rate of their IT development and modernization efforts.

Even with the numerous project failures, the role of information technology continues to grow in importance to organizations. "Over the past four decades the role of information technology has evolved from a primarily supporting role to an increasingly strategic role."⁵ This phenomenon can be found in the civilian market place, Federal Government, DoD, and the Army. The trend is expected to continue.

Creation of the CIO Organization

As organizations realized the potential value of their information technology resources, they began to create executive positions known as the CIO. The CIO often was charged with the responsibility of overseeing information technology resources from an enterprise perspective. Again, the executive agencies of the Federal Government followed suite.

In 1996, the President signed what has become known as the Clinger-Cohen Act. It required major Federal Agencies to "establish the position of CIO having clear authority, responsibility and accountability for the Agency's information resources management activities, and providing for greater coordination among the Agency's information."⁶

The Clinger-Cohen Act and the appointment of an Agency CIO was intended to solve a number of problems associated with the acquisition and use of information technology resources. Specifically, the Clinger-Cohen Act was intended to focus attention on the way business processes are conducted and to improve these processes before investing in information technology that supports them. Additionally, the legislation emphasized the need to avoid investments in new systems for which agencies had not adequately planned, which did not work as intended, and did little to improve mission performance. The Act also sought to eliminate the implementation of ineffective information systems.⁷

With the creation of the CIO organization comes the recognition of the increasingly strategic value of the information technology resources in use within the DoD and the Army. To a lesser degree, the appointment of an Army CIO also indicates that the previous attempts to utilize IT to increase the Army's war fighting capabilities have been less than fully successful. But perhaps the most significant realization is the fact that, in order to continue to meet Title X requirements, the Army can not continue to utilize its information technology resources in the same manner it has used them in the past. The Army, as well as many other DoD and Federal

Agencies, can no longer afford to invest in IT without considering the larger enterprise implications.

In fact, the legislation⁸ requires that the Army develop a centralized process for evaluating, selecting, and funding IT projects. The legislation also mandates that in the future the Army must develop systems (both weapon systems and IT systems) that are consistent with approved enterprise architectures (both DoD and Army). These systems must show a significant potential to improve mission performance and/or reduce resource requirements. Lastly, these systems must be both flexible and adaptable.⁹

The Army CIO

Today, a close look at any large-scale user of IT will produce several examples of why that organization needs a CIO. The DoD and the Army are not exceptions to this rule. In 1989, the DoD initiated its Corporate Information Management (CIM) initiative in an attempt to create common information technology systems and save billions of dollars. The anticipated savings were to result from identifying common functional (personnel, logistics, resource management, etc.) requirements across the DoD. With common functional requirements, the acquisition communities would modify existing systems or develop new systems and deploy these systems as replacements for legacy systems. This was a huge undertaking with numerous high-risk activities. The "DoD's CIM initiative included several key aspects: (1) corporate/policy/planning, (2) process and data modeling, (3) process improvement, (4) performance measurement, (5) standard information systems, and (6) computing and communication infrastructure."¹⁰ Of the two approaches to meeting the CIM objectives, namely, (1) select the best systems from the pool of existing systems and then modify them or, (2) reengineer existing processes then apply technology, DoD choose the first. This approach became known as the migration approach. The CIM initiative was riddled with management failures. In its 1997 report, the General Accounting Office (GAO) found the following:

"of the 363 systems that had been selected for migration, 245 systems had never been submitted for review. Additionally, most of the systems that were submitted for this review were approved in the absence of critical technical and programmatic support. Specifically, about 19 percent were approved without supporting technical justification and about 54 percent were approved without documents showing that the functional area had evaluated different options for improving a business area, such as reengineering. Because all of the migration selections submitted for this oversight have been approved—whether adequately supported with technical and programmatic justification or not—this control was essentially meaningless."¹¹

While the Army was not singled out in the GAO report, it shared in the management failures. This is but one example of why the DoD and the Army need strong CIOs.

Roles and Responsibilities

The Clinger-Cohen Act mandated that each Executive Agency establish a Chief Information Officer (CIO) whose primary responsibility would be Information Resources Management. The Secretary of the Army designated the Director of Information Systems for Command, Control, Communications and Computers (DISC4) as the Army CIO on March 19, 1996.¹²

The Secretary identified the primary duties of the CIO as developing, maintaining, and facilitating the implementation of a sound integrated technology architecture for the Army. In addition, the CIO was charged with the responsibilities of effective and efficient design and operation of all major information resources management processes, and monitoring the performance of information technology for the agency. The CIO was also delegated the oversight authority over all Army information systems.

The DISC4 and Army CIO web pages provide additional clarification of the CIO's responsibilities. The CIO web page states the "Army CIO is responsible for all aspects of Army information management and application of information technology to support mission goals."¹³ The DISC4 web page states the CIO "responsibilities include, but are not limited to: the development, maintenance, and facilitation of the implementation of a sound integrated technology architecture for the executive agency; the promotion of effective and efficient design and operation of all major information resource management processes; monitoring the performance of information technology for the agency; and the assessment of positions and personnel necessary to achieve the requirements of the information system."¹⁴

Army Regulation 25-1 states the Army's CIO "responsibilities are: ... principal advisor to the Secretary of the Army and other Army leadership on all information systems. Provide oversight of the Army's collection of information ... information dissemination, ... Integrate the budget, program management, and acquisition decisions affecting information technologies to promote Army efficiency ... Provide the information technology management strategic planning perspective to the Army strategic planning process to include alignment of the IT investment strategy with Army strategic vision, goals, and objectives ... Develop and implement IT performance measurements ... Establish and implement Army-wide IT architecture."¹⁵

The General Services Administration, in its Guide to Planning, Acquiring, and Managing Information Technology Systems, defined the "responsibilities of the CIO as: providing advice and assistance to the head of the agency and other senior agency management personnel to ensure that information technology is acquired and managed in accordance with law. Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency. Promoting the effective and efficient design and operation of all major information resource management processes for the executive agency, including improvements to the work processes."¹⁶

Changes Since Implementation

CIO Vision: An Army that works better and costs less through the smart use of information and information technology.

—LTG Peter M. CuvIELLO

In 1996, the Office of the Director of Information Systems for Command, Control, Communications and Computers was reconfigured in order to satisfy the requirements of the Clinger-Cohen Act and meet the additional responsibilities resulting from the Secretary of the Army's designation of the DISC4 as the Army CIO. The reorganization included integrating the additional requirements resulting from the Clinger-Cohen Act (acquisition oversight and architecture) into the existing DISC4 structure. In cases where it was not appropriate to attempt to integrate the new requirements within the existing DISC4 structure, separate offices (CIO Integration Directorate for example) were created.

Since the DISC4 restructuring, a number of positive changes have occurred as a result of the increased emphasis on managing the Army's IT resources. The DISC4/CIO has updated a number of policies and regulations associated with the Army Enterprise Architecture, Knowledge Management, Acquisition Oversight, and IT Performance Management. The DISC4/CIO continues to refine the IT investment process and the C4/IT investment portfolio, update the Army Enterprise Architecture, and actively participates in the requirement development and prioritization process.¹⁷

While significant progress has been made in each of these areas, more remains to be done in order to achieve LTG CuvIELLO's Vision.

Role of the CIO in Commercial Organizations

To provide technology vision and leadership for developing and implementing IT initiatives that create and maintain leadership for the enterprise in a constantly changing and intensely competitive marketplace.

—Mission of the CIO, Gartner Group Inc.

In many commercial organizations the role of the CIO is gradually changing from one that was focused on technology planning and implementation to one which is focused on strategic issues. In its 1998 study of 340 information technology directors, Kron/Ferry International showed that "the role of the CIO was moving from technical planning and implementation to strategic planning."¹⁸ In addition, Kron/Ferry concluded that as IT was increasingly seen as a key to future business, the CIO increasingly became a more important voice in strategic matters.¹⁹

In a study of 1400 members of Gartner's Executive Programs, Gartner Group found "enterprises are placing executives with significant IT responsibilities at higher levels of executive decision making."²⁰ Gartner went on to state the priorities of the CIOs as "energizing, enabling, executing, and exploiting."²¹

The two studies and much of the trade press seem to present a common picture. As organizations become more dependent on IT, they are increasingly placing greater management attention on both the strategic direction of IT within the organization and the need to continue to exploit its capabilities in order to maintain a competitive advantage. This can be found in companies such as General Motors, General Electric, Xerox, and Amoco. Given the complexities of managing the IT function, these companies have split the task of managing information technology between the CIO and divisional information officers. In this type of structure, the CIO is charged with the responsibility of providing a corporate vision for the use of information technology and the divisional information officers (DIO) are responsible for the development, implementation, and day-to-day management of information systems that support the specific needs of the respective business unit.

Using an IT management approach which focuses on centralized planning with decentralized execution enables organizations to provide a coherent IT vision, via the CIO, while at the same time allowing the various business units, via the DIO, to focus on the specific needs of their respective organization. In this type of situation the DIOs are accountable to both the head of the respective business unit and the CIO. Specifically the DIO is charged with adding value to the business unit by using IT to enhance the business unit's capabilities. The

DIO is also required to adhere to the enterprise architectural standards and management policies established by the CIO.

On a larger scale, the CIO is responsible for establishing a coherent strategic information architecture plan, which is linked to the enterprise's strategic business plan. Ultimately both the respective business managers and the CIO are accountable for the use of IT resources to support the organization.

An alternative to the centralized planning with decentralized execution IT management approach is one which focuses on centralization of all IT activities. Under this type of approach, the CIO is ultimately responsible for the centralized planning, resourcing, and utilization of the organization's IT resources.

Regardless of the how organizations choose to implement a CIO structure, the CIO and supporting staff are typically charged with the responsibility of technology planning, enterprise software applications development and maintenance, IT infrastructure development and maintenance, IT architecture, establishing strategic relationships with key IT suppliers and consultants, IT training, and ultimately adding value to the organization by linking the use of IT resources to the respective business.

Lessons from Civilian Practices

Much of the literature concerning the success or failure of CIOs in commercial organization places great emphasis on where the office of the CIO is located on the organization chart. There have been countless articles published which expose the idea that if the CIO does not report directly to the Chief Executive Officer (CEO) the CIO is destined for failure. But more important than the statements made concerning the significance of the where in the organizational hierarchy the CIO exists, is the seemingly uniform agreement concerning the significance of the relationship between the CIO, CEO and other members of the executive management team. While the literature suggests that many CIOs have not had the impact on the organization's bottom line that the senior management team had desired, they are nonetheless having a positive impact on the organization's capabilities. The ability of CIOs to establish themselves as part of the top management team, implement a coherent IT architecture, and link the use of the organization's IT resources to the organization's business are all key attributes of successful CIO organizations.

The CIO's ability to establish a peer relationship with the organization's senior management team is often viewed as key to his or her ability to effectively influence how the

organization views the strategic value of its IT resources. When not seen as a member of the senior management team, the CIO has difficulty building the organizational alliances necessary to implement sound IT investment strategies and has limited success in bringing the IT strategic direction in line with the organization's long term goals.

An additional attribute of successful CIO organizations is their ability to define and implement a flexible IT architecture. The significance of implementing a sound architecture cannot be overstated. Successful organizations use their IT architecture as a basis for evaluation of a variety of activities ranging from planning to investment decisions. Without a robust IT architecture (and the infrastructure it describes) organizations find it difficult to share information electronically, and may experience numerous problems when attempting to integrate new or changed business requirements within existing electronic processes.

Perhaps the most significant of the key attributes of successful CIO organizations is the ability to link the use of the organization's IT resources to the organization's business objectives. In many organizations this is done by creating an environment that involves the CIO in the development of business plans and the functional owner in the decision process concerning the expenditure of IT resources. In this situation, the CIO is forced to develop an understanding of the issues facing the business unit in order to advise the business unit of the advantages and disadvantages of the potential courses of action. Conversely, the business unit is forced to weigh the cost of the potential solutions against the overall value created by the IT investment.

Implications of Current IT Policies on Transformation

Technological change may well revolutionize the manner in which the United States conducts and sustains military operations in the 21st century. But to do this requires utilizing information technology in such a way as to provide both accurate and timely information at an affordable price. As the Army embarks on transforming itself into a force that is lighter, more lethal, and more sustainable, it realizes doing so requires it to look to information technology as a key enabler. This also requires the Army to look at ways to combine the efficiencies associated with the ongoing Revolution in Business Affairs with the ongoing changes associated with the Revolution in Military Affairs. If the Army hopes to be successful in this endeavor, it must change many of the existing policies and perceptions concerning how it identifies, acquires, and implements information technology.

Current IT Policies

Within the Army, acquisition programs are approved and resourced based on operational needs. The proposed system must have a clearly identified advocate and user. In order for the system to be developed and implemented it must meet numerous operational requirements, deal with existing resource limitations, and comply with existing acquisition policies. While this process has worked in the past, its future viability is questionable due to the rapid pace of technological change and increased reliance on commercial products.

Once a system reaches the sustainment phase of its operational life-cycle, it must be maintained. But the ability to affect significant architectural change once a system is fielded is severely limited due to the size, complexity, desire to maintain commonality within the system, and need for interoperability.

The recognized need to continue to develop new, more effective systems (both weapons and information) while maintaining existing ones, creates a unique challenge for the Army CIO. If the Army hopes to avoid the problems associated with the DoD CIM initiative²² and the difficulties of achieving year 2000 compliance, then the Army CIO must continue to pursue cross functional ownership of its IT resources, continue to invest in centralized planning and control, and continue to develop a common IT infrastructure.

Cross Functional Ownership

"Today we live in a world where information superiority is critical to our survival."²³ Due to the resource constraints (time, people, and funding) and the need for greater information, we are faced with the need to make more informed choices concerning the weapons and information systems we choose to develop, implement, and maintain. While the current budgeting and prioritization processes embraces the concept of cross-functional representation, it allows for the procurement of information systems under the auspices of each Program Evaluation Group (PEG). As a result, the ability to accurately resource, implement, and maintain a flexible IT architecture and common infrastructure is severely limited. This is due in part to the existing annual funding cycle used within DoD, as well as the ever-changing resourcing priorities within each PEG.

The existing process allows each functional area (operations, logistics, personnel, etc.) to submit requirements for new or enhanced systems to the appropriate reviewing organization. Once recognized, the requirement is eventually prioritized and resourced based on need. Once

resourced, the requirement is forwarded to the appropriate acquiring organization, and so on until a system that satisfies the need is implemented. While this is an oversimplification of a complex process, it reflects the basic steps.

The resulting effect of this process is a general lack of awareness concerning the value of the information generated by the respective system when shared across functional lines of responsibility and of the cost associated with creating and managing it. This lack of awareness only complicates the task of resourcing and maintaining the respective system and the associated infrastructure that supports it. The resulting affect is an annual cycle of controlled chaos, during which the funding needs of each system are explained in terms of new operational capabilities or the creation of operational deficiencies if the resources are not provided.

While this process provides the Army the opportunity to annually review its allocation of resources, it has also allowed it to systematically postpone technology refreshment of key IT resources until they are on the verge of failure. The allocation of resources dedicated to achieving year 2000 compliance is an example of this fact.

As the Army seeks to transition to the objective force, the Army CIO must ensure the CIO Office has not only the cross functional ownership for the IT systems in use, but also cross functional ownership of the underlying infrastructure and generation of the organizational commitment to maintain it. Otherwise, the Army's ability to consistently provide reachback and split-based operations will be severely limited.

Centralized Planning, Control, and Resourcing

Today our information systems are becoming so intertwined that changes in one system can have second and third order affects in another. For example, a regional data processing center upgrades its computer's operating system from ABC1 to ABC1.1 (only a minor change according to the product's vendors). The data center conducts the appropriate operational test and all systems work as documented. Three months later version 2 of application 123 is shipped to the center with instructions to load the upgrade. Personnel from the data center attempt to install the software upgrade but are unsuccessful. In the meantime, a number of other applications that run on the same computers as application 123 have been modified to take advantage of the new capability offered by ABC1.1 and will no longer run on version ABC1 of the operating system. Unfortunately, neither the data center nor the organization maintaining the 123 software application has the resources necessary to make the operating system and

123 software application compatible. While fictional, this example illustrates how one seemingly simple change can have significant operational impacts. The IT resources used within the Army have suffered from very similar circumstances.

The disconnects concerning the various operational capabilities of information systems (and their underlying Infrastructure) within the Army point to a renewed need for centralized planning and control concerning the use of IT resources. The implications of continually changing priorities combined with the pace of technological change requires the Army to pay greater attention to resourcing, planning, and executing technology upgrades in order to maintain interoperability.

Common IT Infrastructure

Commonality: A quality which applies to materiel or systems possessing like and interchangeable characteristics enabling each to be utilized or operated and maintained by personnel trained on the others without additional specialized training; and/or having interchangeable repair parts and/or components.

— Defense Systems Management College

To support present and future requirements, the Army needs a common and coordinated IT infrastructure. The Army's IT infrastructure provides the basic foundation for the development and management of the information systems and information products which the Army has become dependent upon. Yet, infrastructure development and maintenance is an area that has continually been under-resourced, with the resulting need for installations to create and maintain their own IT infrastructure as best they can.

But, as the systems become more complex and interdependent, it becomes more costly and more difficult to manage and sustain multiple versions of the same or similar products. This has been demonstrated repeatedly in commercial industry and the Federal Government. The "September, 1999 version of the Federal Enterprise Architecture Framework estimated that organizations which chose to pursue an enterprise architecture using a systems approach, rather than a resourced approach, expends 26 times more resources than those which used the resourced approach."²⁴

If this estimate proves to be true, the Army will find it very difficult, time consuming, and very costly to link the activities associated with the Revolution in Business Affairs with the Revolution in Military Affairs if it does not change the method in which it sustains its IT

infrastructure. In today's dynamic global environment, as technology advances and operational requirements change, the IT infrastructure must be constantly updated in order to provide a basis for future change.

Conclusion

In the past the Army has had ample time to adapt technology to military use. However, due to the pace of technological change, it is more important than ever before that both political and military leaders pay special attention to the adaptation of information technology to military specific purposes in order to maintain a competitive advantage. Accurate, timely, and relevant information has always been highly sought after by military planners and leaders. Today, advances in technology have made vast amounts of information relatively inexpensive and readily available. Improvements in the manner in which information is processed and presented to military leaders may prove to be the deciding factor in future military conflicts. It is because of these facts that the Army must place greater emphasis on information and the responsibilities of those who manage it. It must continue to work to develop a cross functional sense of ownership for its IT resources, continue to make an extraordinary effort to synchronize the change processes associated with operating and maintaining its information management systems, and recognize the importance of providing a common IT infrastructure to the enterprise.

WORD COUNT = 4891

ENDNOTES

¹"Army Announces Vision of the Future," 12 October 1999; available from <<http://www.dtic.mil/armylink/news/Oct1999/r19991015vision095.html>>; Internet; accessed 20 September 2000.

²Louis Caldera and Eric K. Shinseki. United States Army Posture Statement FY01, The Army – Soldiers On Point for the Nation ... Persuasive in Peace, Invincible in War. Posture Statement presented to the 106th Cong., 2d sess. (Washington, D.C.: U.S. Department of the Army, 2000), 15.

³Delores M. Etter, "Spiral Workshop," 13 September 2000; available from <<http://www.sei.cmu.edu/cbs/spiral2000/september/Etter.ppt>>; Internet; accessed 26 September 2000.

⁴"CHAOS: A Recipe For Success," 1995; available from <<http://standishgroup.com/visitor/chaos.htm>>; Internet; accessed 25 September 2000.

⁵Detlev H. Smaltz, "Antecedents of CIO Effectiveness: A Role-Based Perspective" (Ph.D. diss., Florida State University, 1999), 1.

⁶"Clinger-Cohen Act of 1996 And Related Documents," May 2000; available from <<http://www.c3i.osd.mil/org/cio/doc/CCA-Book-Final.pdf>>; Internet; accessed 27 September 2000.

⁷Ibid.

⁸The Government Performance and Results Act and the Information Technology Management Reform Act.

⁹In this context flexibility addresses the capability to insert or update obsolete technology components. Adaptability describes the ability to add or extend system functionality.

¹⁰General Account Office, Defense IRM – Poor Implementation of Management Controls Has Put Migration Strategy at Risk (Washington, D.C.: U.S. General Accounting Office, October 1997), 2.

¹¹Ibid, 6.

¹²"Chief Information Officer of the Army Implementation Plan", approved 16 July 1997; available from <http://www.army.mil/disc4/cio/imp_plan.htm>; Internet; accessed 30 November 2000.

¹³Army Chief Information Officer Web Page, 25 August 2000; available from <<http://www.army.mil/disc4/cio/>>; Internet; accessed 2 October 2000.

¹⁴"Chief Information Officer Responsibilities," 4 August 2000; available from <<http://www.army.mil/disc4/overview/responsibilities.html>>; Internet; accessed 2 October 2000.

¹⁵Department of the Army, Army Information Management, Army Regulation 25-1 (Washington, D.C.: U.S. Department of the Army, 15 February 2000), 3.

¹⁶General Services Administration, A Guide to Planning, Acquiring, and Managing Information Technology Systems, Version 1 December 1998 (Washington, D.C.: General Services Administration, 1998), 2-25.

¹⁷Patricia Bodenstein <Patricia.Bodenstein@HQDA.Army.Mil>, "Army CIO Overview," electronic mail message sent to Bobby McKinnon <blm@andrew.cmu.edu>, 30 November 2000.

¹⁸"The Changing Role of the Chief Information Officer." 25 February 2000; available from <www.cio.com/forums/executives/kronferry_content.html>; Internet; access 14 December 2000.

¹⁹Ibid.

²⁰Carol Wallace, "Gartner Identifies Major Shifts in Chief Information Officer Roles." 13 June 2000; available from <<http://www.gartner.com/public/static/aboutgg/pressrel/pr20000612a.html>>; Internet; accessed 14 December 2000.

²¹Ibid.

²²As documented in the "General Account Office , Defense IRM – Poor Implementation of Management Controls Has Put Migration Strategy at Risk (Washington, D.C.: U.S. General Accounting Office, October 1997)".

²³Jacques S. Gansler, "Competition By Design: Building Affordable Weapon Systems for the 21st Century." 1 June 1998. Available from <http://www.acq.osd.mil/ousda/speech/pro-services_council.html>; Internet; accessed 8 February 2001.

²⁴Federal Chief Information Officers Council. "Federal Enterprise Architecture Framework Version 1.1" September 1999. Available from <<http://www.itpolicy.gsa.gov/mke/archplus/fedarch1.pdf>>; Internet. accessed 11 January 2001.

BIBLIOGRAPHY

- Association for Federal Information Resources Management. "The Federal CIO: A Seat at the Table." June 1996. Available from <<http://www.affirm.org/Pubs/wpapers/CIOSeat.htm>>. Internet. Accessed 14 December 2000.
- "Army Announces Vision of the Future." 12 October 1999. Available from <<http://www.dtic.mil/armylink/news/Oct1999/r19991015vision095.html>>. Internet. Accessed 20 September 2000.
- Army Chief Information Officer Web Page. 25 August 2000. Available from <<http://www.army.mil/disc4/cio/>>. Internet. Accessed 2 October 2000.
- Bodenstein, Patricia <Patricia.Bodenstein@HQDA.Army.Mil>, "Army CIO Overview," Electronic mail message sent to Bobby McKinnon <blm@andrew.cmu.edu>. 30 November 2000.
- Caldera, Louis, and Eric K. Shinseki. United States Army Posture Statement FY01, The Army – Soldiers On Point for the Nation ... Persuasive in Peace, Invincible in War. Posture Statement presented to the 106th Cong., 2d sess. Washington, D.C.: U.S. Department of the Army, 2000.
- "CHAOS: A Recipe For Success." 1995. Available from <<http://standishgroup.com/visitor/chaos.htm>>. Internet. Accessed 25 September 2000.
- "Clinger-Cohen Act of 1996 And Related Documents." May 2000. Available from <<http://www.c3i.osd.mil/org/cio/doc/CCA-Book-Final.pdf>>. Internet. Accessed 27 September 2000.
- Etter, Delores M., "Spiral Workshop." 13 September 2000. Available from <<http://www.sei.cmu.edu/cbs/spiral2000/september/Etter.ppt>>. Internet. Accessed 26 September 2000.
- Federal Chief Information Officers Council. "Federal Enterprise Architecture Framework Version 1.1" September 1999. Available from <<http://www.itpolicy.gsa.gov/mke/archplus/fedarch1.pdf>>. Internet. Accessed 11 January 2001.
- Field, Tom. "The CIO Role – Great Expectations." 1 June 1998. Available from <http://www.cio.com/archive/060198_great_content.html>. Internet. Accessed 19 December 2000.
- Frank, Diane. "Building a blueprint for agency CIOs: GAO, congressmen call for stronger management role for federal CIOs." 3 April 2000. Available from <<http://www.fcw.com/print.asp>>. Internet. Accessed 29 August 2000.
- . "CIOs need status, support." 27 March 2000. Available from <<http://www.fcw.com/print.asp>>. Internet. Accessed 29 August 2000.
- Kapil Kak, Dy. "Revolution in Military Affairs—An Appraisal." Available from <<http://www.idsa-india.org/an-apr-01.html>>. Internet. Accessed 14 December 2000.

Paul, Lauren Gibbons. "A Separate Piece." 15 October 1998. Available from <http://www.cio.com/archive/101598_cover_content.html>. Internet. Accessed 8 January 2001.

Seffers, George I. "Air Force rebuilding." 17 August 2000. Available from <<http://www.fcw.com/print.asp>>. Internet. Accessed 29 August 2000.

Shelton, Henry H. "JOINT VISION 2020." June 2000. Available from <<http://www.dtic.mil/jv2020/jvpub2.htm>>. Internet. Accessed 26 September 2000.

Sifonis, John G. and Beverly Goldberg. "Strategic Management – Changing Role of the CIO – As technology becomes central to business, the CIO becomes a key mover in the ranks of upper management." 24 March 1997. Available from <<http://www.techweb.com/se/directlink.cgi?IWK19970324S0043>>. Internet. Accessed 19 December 2000.

Smaltz, Detlev H. "Antecedents of CIO Effectiveness: A Role-Based Perspective." Ph.D. diss., Florida State University, 1999.

Swanson, Sandra ND Elisabeth Goodridge. "Who's In Charge of IT? Managing IT is as much about business as it is about technology." 16 October 2000. Available from <<http://www.informationweek.com/shared/printArticle?article=infoweek/808/prmanage.htm&pub=iwk>>. Internet. Accessed 14 December 2000.

"The Changing Role of the Chief Information Officer." 25 February 2000. Available from <www.cio.com/forums/executives/kronferry_content.html>. Internet; Access 14 December 2000.

U.S. Department of the Army, Army Information Management. Army Regulation 25-1. Washington, D.C.: U.S. Department of the Army, 15 February 2000.

U.S. General Account Office, Defense IRM – Poor Implementation of Management Controls Has Put Migration Strategy at Risk. Washington, D.C.: U.S. General Accounting Office, October 1997.

U.S. General Services Administration. A Guide to Planning, Acquiring, and Managing Information Technology Systems, Version 1 December 1998. Washington, D.C.: General Services Administration, Office of Governmentwide Policy, Emerging Information Technology Policies Division, 1998.

Wallace, Carol. "Gartner Identifies Major Shifts in Chief Information Officer Roles." 13 June 2000. Available from <<http://www.gartner.com/public/static/aboutgg/pressrel/pr20000612a.html>>. Internet. Accessed 14 December 2000.